

A NOTE ON THE ALGEBRA OF P-ADIC MULTI-ZETA VALUES

SINAN ÜNVER

Abstract. We prove that the algebra of p-adic multi-zeta values, as defined in [4] or [2], are contained in another algebra which is defined explicitly in terms of series. The main idea is to truncate certain series, expand them in terms of series all of which are divergent except one, and then take the limit of the convergent one. The main result is Theorem 3.0.27.

1. INTRODUCTION

Multi-zeta values were defined by Euler as the sum of the series:

$$\zeta(s_1, s_2, \dots, s_k) := \sum_{0 < n_1 < \dots < n_k} \frac{1}{n_1^{s_1} n_2^{s_2} \dots n_k^{s_k}},$$

for $s_1, \dots, s_{k-1} \geq 1$ and $s_k > 1$. The Euler-Kontsevich formula [3] expresses these numbers in terms of iterated integrals on the thrice punctured line $X := \mathbb{P}^1 \setminus \{0, 1, \infty\}$. This formula interprets multi-zeta values as real periods of the mixed Tate motive coming from the unipotent fundamental group of X [1], [3]. These imply many relations between the multi-zeta values and the algebra of these values has arithmetic significance as it relates to the tannakian fundamental group of mixed Tate motives over \mathbb{Z} [3].

The p-adic version of these values were defined by Deligne (unpublished, explained in [4]) coming from the comparison theorem between the de Rham and the crystalline fundamental group of X . The double shuffle relations for these values were proved by Furusho and Jafari and the Drinfel'd-Ihara relations were proved by the author. The question of algebraic independence or even non-vanishing seems to be a more difficult question. We do not even know that $\zeta_p(2k+1)$ are non-zero for all primes p , and positive integers k . This suggests that in order to prove linear independence among these numbers one might need a somewhat more explicit description of these numbers or the algebra generated by these numbers. This paper is a first attempt in this direction. Our aim in this note is to prove that the algebra of p-adic multi-zeta values lie in another algebra that is described only using certain series. The remaining, but more difficult question is to study these series.

It turns out that the individual truncated series that appear in the expression for p-adic multi-zeta values are divergent, but their certain linear combinations converge. The main idea is to consider these divergent series and express them as linear combinations of a convergent series and other divergent series and then take the convergent part. We call this process the *regularization* of the series.

In §2, we describe this process. The main point is that there are certain simple divergent series which we denote by $\sigma_p(\underline{s})$, which are linearly independent under the algebra of *power series functions*. That these series are linearly independent is proved in Proposition 2.0.3; the fact that all the series we are interested can be

expressed in terms of these divergent series is proved in Proposition 2.0.7. Next in Proposition 2.0.14, which forms the basis for the inductive arguments, we prove that, under conditions that are satisfied by the series that appear below, if the truncated series that are the coefficients of a power series are regular then so are the coefficients of its antiderivative after it is multiplied by one of the forms ω_i .

In §3, we apply the above results to the truncated series that appear in the expressions for p-adic multi-zeta values. The main idea is based on the results of [4]. Namely, using the standard lifting of Frobenius on X , which is a good choice outside a disc of radius 1 around 1, we obtain a differential equation (3.0.3) for \mathbf{g} . Next we use [4, Proposition 2] to find an expression for the value of \mathbf{g} at infinity and the relation (3.0.2) to relate that value to g , whose coefficients are the p-adic multi-zeta values. The main result is Theorem 3.0.27 where we prove that the algebra of p-adic multi-zeta values \mathcal{Z} lie inside the algebra \mathcal{P} of values of regularized series. Finally, we note in Remark 3.0.28 that the above result also implies the same statement for the p-adic multiple zeta values as defined by Furusho [2], since the algebra that they generate is the same as \mathcal{Z} .

Acknowledgements. The author thanks T. Terasoma for a very short discussion which became the main inspiration for this note.

2. ITERATED SUMS

Fix a prime p . For $\underline{s} := (s_1, \dots, s_k)$, with $0 \leq s_i$, and $\underline{m} := (m_1, \dots, m_k)$, with $0 \leq m_i < p$, let

$$\sigma(\underline{s}; \underline{m})(n) := \sum \frac{1}{n_1^{s_1} \dots n_k^{s_k}},$$

where the sum is over $0 < n_1 < n_2 < \dots < n_k < n$ with $p|(n_i - m_i)$. Similarly, we let $\gamma(\underline{s}; \underline{m})(n) := n^{-s_k} \cdot \sigma(\underline{s}'; \underline{m}')(n)$, if $p|(n - m_k)$ and 0 otherwise, where $\underline{s}' = (s_1, \dots, s_{k-1})$ and $\underline{m}' = (m_1, \dots, m_{k-1})$. Let $\sigma_p(\underline{s})(n) := \sigma(\underline{s}; \underline{0})(n)$, where $\underline{0} = (0, \dots, 0)$. We define the *depth* as $d(\underline{s}) = k$ and the *weight* as $w(\underline{s}) := \sum s_i$.

Let us call a function $f : \mathbb{N}_{\geq n} \rightarrow \mathbb{Q}_p$, for some n , a *power series function*, if there exist power series $p_i(x) \in \mathbb{Q}_p[[x]]$, which converge on the closed unit disc $D(r_i)$ around 0, for some $r_i > |p|$, for $0 \leq i < p$, such that $f(a) = p_i(a - i)$ for all $a \geq n$ and $p|(a - i)$. Clearly there is a unique power series function \bar{f} with domain $\mathbb{Z}_{\geq 0}$ such that \bar{f} restricts to f on $\mathbb{N}_{\geq n}$. We let $f(0) := \bar{f}(0)$, or more explicitly $f(0) = \lim_{k \rightarrow 0} f(k)$. We will identify two power series functions if they are the same on the intersection of their domains of definition. Note that we have the following [5, Proposition 5.0.5]:

Proposition 2.0.1. (i) *The product and sum of power series functions are also power series functions. So is the function defined as $f(n) = n^s$, if $p \nmid n$; and $f(n) = 0$, if $p|n$, for $s \in \mathbb{Z}$.*

(ii) *If f is a power series function, let us define $f^{[1]}$ and $f^{(1)}$ as $f^{[1]}(n) = f^{(1)}(n) = (f(n) - f(0))/n$, if $p|n$; $f^{[1]}(n) = 0$, $f^{(1)}(n) = f(n)/n$, if $p \nmid n$. Then both $f^{[1]}$ and $f^{(1)}$ are power series functions.*

(iii) *If $f : \mathbb{N}_{\geq n_0} \rightarrow \mathbb{Q}_p$ is a power series function and if we define*

$$F(n) := \sum_{n_0 \leq k \leq n} f(k),$$

then so is F .

The following lemma on power series will be essential while we are proving the linear independence of the σ_p 's.

Lemma 2.0.2. *Let $f, g \in \mathbb{Q}_p[[z]]$ be two power series which are convergent on $D(a)$, for some $a > 1$. Suppose that $g \neq 0$, and let $h := f/g$. If there exist $C_i \in \mathbb{Q}_p$ and $n \geq 1$ such that $h(z+1) - h(z) = \frac{C_n}{z^n} + \cdots + \frac{C_1}{z}$, for infinitely many $z \in D(a)$ then h is constant and $C_i = 0$, for all i .*

Proof. By the Weierstrass preparation theorem, if the above equality holds for infinitely many $z \in D(a)$ then it holds for all $z \in D(a)$, except for the zeros of the denominators involved. Suppose that $f \neq 0$, then again by the Weierstrass preparation theorem there are polynomials $p, q \in \mathbb{Q}_p[z]$, and power series $u, v \in \mathbb{Q}_p[[z]]$, which converge and are nonzero on $D(a)$ such that $f = p \cdot u$ and $g = q \cdot v$. Therefore the poles of $h(z)$ and $h(z+1)$ in $D(a)$, together with their multiplicities, are exactly those of $p(z)/q(z)$ and $p(z+1)/q(z+1)$. Let $\mathfrak{P}(k)$ denote the set of poles of k in $D(a)$.

Then

$$\mathfrak{P}(h) \Delta (\mathfrak{P}(h) - 1) \subseteq \mathfrak{P}\left(\frac{C_n}{z^n} + \cdots + \frac{C_1}{z}\right) \subseteq \mathfrak{P}(h) \cup (\mathfrak{P}(h) - 1),$$

where Δ denotes the symmetric difference.

If $C_i \neq 0$ for some i , then $\mathfrak{P}\left(\frac{C_n}{z^n} + \cdots + \frac{C_1}{z}\right) = \{0\}$, hence $\mathfrak{P}(h) \neq \emptyset$. This implies that $\mathfrak{P}(h) \neq \mathfrak{P}(h) - 1$. Since $|\mathfrak{P}(h)| = |\mathfrak{P}(h) - 1|$ is finite, this implies that the symmetric difference of $\mathfrak{P}(h)$ and $\mathfrak{P}(h) - 1$ contains at least two elements. This is a contradiction. Hence $C_i = 0$, for all i . This implies that $h(z+1) = h(z)$. Choosing an α where h does not have a pole and replacing h with $\bar{h} := h - h(\alpha)$, we see that \bar{h} has infinitely many zeros in $D(a)$ and hence is 0. \square

Let \mathcal{P} denote the algebra of power series in \mathbb{Q}_p which converge on $D(r)$ for some $r > |p|$. We will identify these power series with the functions that they define from $p\mathbb{N}$ to \mathbb{Q}_p . Let $\sigma_p(\emptyset) := 1$. Let \mathcal{P}_σ denote the module over \mathcal{P} generated by $\sigma_p(\underline{s})$ with $\underline{s} \in \cup_n \mathbb{N}^{\times n}$. Then by the shuffle product formula for series, \mathcal{P}_σ is an algebra.

Proposition 2.0.3. *The algebra \mathcal{P}_σ is free with basis $\{\sigma_p(\underline{s}) | \underline{s} \in \cup_n \mathbb{N}^{\times n}\}$ as a module over \mathcal{P} .*

Proof. By induction on m we will show the linear independence of the set $S_m := \{\sigma_p(\underline{s}) | d(\underline{s}) \leq m\}$. For any function $f : p\mathbb{N} \rightarrow \mathbb{Q}_p$, we let $\delta(f)$ denote the function defined by $\delta(f)(n) := f(n+p) - f(n)$. Note that

$$\delta \sigma_p(\alpha_1, \dots, \alpha_{m+1})(n) = \frac{1}{n^{\alpha_{m+1}}} \sigma_p(\alpha_1, \dots, \alpha_m)(n).$$

We know the linear independence for the set $S_0 = \{1\}$. Assuming that we know the linear independence for S_m , we will prove it for S_{m+1} . Let us suppose that $\{\sigma_p(\alpha_1, \dots, \alpha_{m+1})\} \cup S_m$ is linearly dependent over \mathcal{P} . Then we have an expression of the form

$$\sigma_p(\alpha_1, \dots, \alpha_{m+1}) = \sum_{d(\alpha) \leq m} a_\alpha \sigma_p(\alpha),$$

with a_α a quotient of elements in \mathcal{P} .

Applying δ to the last equation we get

$$\frac{1}{z^{\alpha_{m+1}}} \sigma_p(\alpha_1, \dots, \alpha_m) = \sum_{d(\alpha)=m} \delta(a_\alpha) \sigma_p(\alpha) + \sum_{d(\alpha)<m} b_\alpha \sigma_p(\alpha).$$

The induction hypothesis implies that $\frac{1}{z^{\alpha_{m+1}}} = \delta(a_{\alpha_1 \dots \alpha_m})$, and this contradicts the lemma above.

Next we do an induction on the number of elements $\sigma_p(\alpha)$ with $d(\alpha) = m + 1$, and $a_\alpha \neq 0$. Suppose that we have a non-trivial equation

$$\sum_{d(\alpha) \leq m+1} a_\alpha \sigma_p(\alpha) = 0.$$

By the induction assumption on m , there is a $\beta = (\alpha_1, \dots, \alpha_{m+1})$ such that $a_\beta \neq 0$. Dividing by this and rearranging we get

$$\sigma_p(\beta) + \sum_{\substack{d(\alpha)=m+1 \\ \alpha \neq \beta}} b_\alpha \sigma_p(\alpha) = \sum_{d(\alpha) \leq m} b_\alpha \sigma_p(\alpha),$$

where b_α are quotients of power series functions. Applying δ to this equation and using induction on the number of $b_\alpha \neq 0$ with $d(\alpha) = m + 1$ we obtain $\delta(b_\alpha) = 0$ for all α with $d(\alpha) = m + 1$, hence these b_α are constant and equal to, say c_α .

So the last equation can be rewritten as

$$\sigma_p(\beta) + \sum_{\substack{d(\alpha)=m+1 \\ \alpha \neq \beta}} c_\alpha \sigma_p(\alpha) = \sum_{d(\alpha) \leq m} b_\alpha \sigma_p(\alpha),$$

applying δ we obtain that

$$\frac{1}{z^{\alpha_{m+1}}} + \sum_{\substack{k \in \mathbb{N} \\ k \neq \alpha_{m+1}}} c_{(\alpha_1, \dots, \alpha_m, k)} \frac{1}{z^k} = \delta(b_{(\alpha_1, \dots, \alpha_m)}).$$

The above lemma again gives a contradiction. \square

Let \mathcal{F} denote the algebra of power series functions and $\iota \in \mathcal{F}$ denote the function that sends n to n . Let $\mathcal{F}(\frac{1}{\iota})$ be the algebra obtained by inverting ι . Note that ι is already invertible on the components $i + p\mathbb{N}$ with $0 < i < p$. Let \mathcal{F}_σ be the module over \mathcal{F} generated by $\sigma_p(\underline{s})$ with $\underline{s} \in \cup_n \mathbb{N}^{\times n}$. Then by the shuffle product formula for series, \mathcal{F}_σ is an algebra. Let $\mathcal{F}_\sigma(\frac{1}{\iota}) = \mathcal{F}_\sigma \otimes_{\mathcal{F}} \mathcal{F}(\frac{1}{\iota})$.

Corollary 2.0.4. *The algebra \mathcal{F}_σ (resp. $\mathcal{F}_\sigma(\frac{1}{\iota})$) is free with basis $\{\sigma_p(\underline{s}) | \underline{s} \in \cup_n \mathbb{N}^{\times n}\}$ as a module over \mathcal{F} (resp. $\mathcal{F}(\frac{1}{\iota})$).*

Definition 2.0.5. Let $\mathfrak{r} : \mathcal{F}_\sigma \rightarrow \mathcal{F}$ denote the projection with respect to the above basis. We will denote the projection $\mathcal{F}_\sigma(\frac{1}{\iota}) \rightarrow \mathcal{F}(\frac{1}{\iota})$ by the same notation. Similarly, let $\mathfrak{s} : \mathcal{F}(\frac{1}{\iota}) \rightarrow \mathcal{F}$ denote the projection that has the effect of deleting the principal part of the Laurent series expansion for the component $p\mathbb{N}$, and is identity on the components $i + p\mathbb{N}$ with $0 < i < p$.

Let $\underline{s} := (s_1, \dots, s_k)$, and $\underline{t} := (t_1, \dots, t_l)$. We write $\underline{t} \leq \underline{s}$ if there exists an increasing function $j : \{1, \dots, l\} \rightarrow \{1, \dots, k\}$ such that $t_i \leq s_{j(i)}$, for all i .

Lemma 2.0.6. *Let f be a power series function and let g be defined as*

$$g(n) = \sum_{0 < a < n} f(a) \sigma_p(\underline{s})(a)$$

for some $\underline{s} := (s_1, \dots, s_k)$. Then

$$g = \sum_{\underline{t} \leq \underline{s}} f_{\underline{t}} \sigma_p(\underline{t}),$$

for some power series functions $f_{\underline{t}}$. Similarly, if h is defined as

$$h(n) := \sum_{\substack{0 < a < n \\ p|a}} \frac{f(a)}{a^s} \sigma_p(\underline{s})(a),$$

for some $s \geq 1$ then

$$h = \sum_{\underline{t} \leq \underline{s}'} f_{\underline{t}} \sigma_p(\underline{t}),$$

for some power series functions $f_{\underline{t}}$, where $\underline{s}' := (s_1, \dots, s_k, s)$.

Proof. We will prove this by induction on $d(\underline{s})$. Suppose that $d(\underline{s}) = 0$ and hence $\sigma_p(\underline{s}) = 1$. Then for g the assertion follows from Proposition 2.0.1. Let $f(z) = \sum_{0 \leq i} b_i z^i$, for $|z| \leq |p|$, then

$$h(n) = b_0 \sigma_p(s)(n) + \dots + b_{p-1} \sigma_p(1)(n) + \sum_{\substack{0 < a < n \\ p|a}} \bar{f}(a),$$

where $\bar{f}(z) := b_p + b_{p+1}z + \dots$. Again the statement follows from Proposition 2.0.1.

Now assume the statement for all \underline{s} with $d(\underline{s}) \leq k$ and fix $\underline{s} := (s_1, \dots, s_{k+1})$. Let F be as in Proposition 2.0.1, then

$$g(n) = F(n-1) \sigma_p(\underline{s})(n) - \sum_{\substack{0 < n_{k+1} < n \\ p|n_{k+1}}} \frac{F(n_{k+1})}{n_{k+1}^{s_{k+1}}} \sigma_p(s_1, \dots, s_k)(n_{k+1})$$

and the statement follows from the induction hypothesis on h .

On the other hand,

$$\begin{aligned} h(n) &= \sum_{\substack{0 < a < n \\ p|a}} \left(\frac{b_0}{a^s} + \dots + \frac{b_{s-1}}{a} + \bar{f}(a) \right) \sigma_p(\underline{s})(a) \\ &= b_0 \sigma_p(\underline{s}, s)(n) + \dots + b_{s-1} \sigma_p(\underline{s}, 1)(n) + \sum_{\substack{0 < a < n \\ p|a}} \bar{f}(a) \sigma_p(\underline{s})(a) \end{aligned}$$

and the statement follows by the statement that we just proved on g . □

Proposition 2.0.7. For any \underline{s} and \underline{m} , $\sigma(\underline{s}; \underline{m}) \in \mathcal{F}_\sigma$.

Proof. We will prove this by induction on $d(\underline{s})$. If $d(\underline{s}) = 1$, then $\sigma(\underline{s}, \underline{m}) = \sigma_p(\underline{s})$ if $m_1 = 0$; and $\sigma(\underline{s}, \underline{m}) \in \mathcal{F}$ otherwise by Proposition 2.0.1. Suppose we know the result for $d(\underline{s}) \leq k$, and fix \underline{s} with $d(\underline{s}) = k+1$.

Let $\underline{s} = (s_1, \dots, s_{k+1})$, $\underline{s}' = (s_1, \dots, s_k)$, $\underline{m} = (m_1, \dots, m_{k+1})$, and $\underline{m}' = (m_1, \dots, m_k)$. Since

$$\sigma(\underline{s}; \underline{m})(n) = \sum_{\substack{0 < a < n \\ p|(a-m_{k+1})}} \frac{\sigma(\underline{s}'; \underline{m}')(a)}{a^{s_{k+1}}},$$

using the induction hypothesis we realize that we only need to show that functions of the form

$$\sum_{\substack{0 < a < n \\ p|(a-m)}} \frac{f(a)}{a^s} \sigma_p(\underline{t})(a),$$

with f a power series function, are in \mathcal{F}_σ and this is exactly the statement of the previous lemma. □

In fact, from the proof above it follows that $\sigma(\underline{s}; \underline{m})$ is an \mathcal{F} -linear combination of $\sigma_p(\underline{t})$ with $\underline{t} \leq \underline{s}$.

Definition 2.0.8. For a function $f \in \mathcal{F}_\sigma$, let $\tilde{f} := \mathbf{r}(f) \in \mathcal{F}$. We call \tilde{f} the *regularization* of f . Since by the previous proposition $\sigma(\underline{s}; \underline{m}) \in \mathcal{F}_\sigma$, we let $\tilde{\sigma}(\underline{s}; \underline{m}) \in \mathcal{F}$ its regularization and $\underline{\sigma}(\underline{s}; \underline{m}) = \lim_{n \rightarrow 0} \tilde{\sigma}(\underline{s}; \underline{m})(n)$.

For a function $f : \mathbb{N} \rightarrow \mathbb{Q}_p$ and $0 \leq m < p$, let $f_{[m]}$ denote the function which is equal to f for values n which are congruent to m modulo p and is 0 otherwise. Recall that $\gamma(\underline{s}; \underline{m})(n) := n^{-s_k} \cdot \sigma(\underline{s}'; \underline{m}')_{[m_k]}(n)$. We will define the regularized version $\tilde{\gamma}(\underline{s}; \underline{m})$ of $\gamma(\underline{s}; \underline{m})$ as follows. If $m_k \neq 0$, then it is defined by $\tilde{\gamma}(\underline{s}; \underline{m})(n) = n^{-s_k} \cdot \tilde{\sigma}(\underline{s}'; \underline{m}')_{[m_k]}(n)$. If $m_k = 0$, and $p(z) = a_0 + a_1 z + \dots$ is such that $\tilde{\sigma}(\underline{s}'; \underline{m}')(n) = p(n)$ for $p|n$, then $\tilde{\gamma}(\underline{s}; \underline{m})(n) = a_{s_k} + a_{s_k+1}n + \dots$, if $p|n$ and 0 otherwise. Finally we let $\underline{\gamma}(\underline{t}; \underline{m}) = \lim_{n \rightarrow 0} \tilde{\gamma}(\underline{t}; \underline{m})(n)$.

Another way to describe this is as follows. For any \underline{s} and \underline{m} , $\gamma(\underline{s}; \underline{m}) \in \mathcal{F}_\sigma(\frac{1}{t})$, and $\tilde{\gamma}(\underline{s}; \underline{m}) := \mathbf{s} \circ \mathbf{r}(\gamma(\underline{s}; \underline{m}))$.

Remark 2.0.9. Note that $\tilde{\sigma}(\underline{s}; \underline{m})^{(n)}(0) = -n! \cdot \underline{\sigma}(\underline{s}, n; \underline{m}, 0) = n! \cdot \underline{\gamma}(\underline{s}, n; \underline{m}, 0)$. The first identity follows from the fact that if $P_k(z)$ is the polynomial such that $P_k(n)$ is the sum of the k -th powers of the first n positive integers then $(z+1)|P_k(z)$, for $k \geq 1$.

Definition 2.0.10. Let \mathcal{P}_w (resp. \mathcal{S}_w , resp. $\tilde{\mathcal{S}}_w$) denote the \mathbb{Q} -space spanned by the $\underline{\sigma}(\underline{s}; \underline{m})$ (resp. $\gamma(\underline{s}; \underline{m})$, resp. $\tilde{\gamma}(\underline{s}; \underline{m})$), with $w(\underline{s}) = w$, and $\mathcal{P} := \sum_w \mathcal{P}_w$ (resp. $\mathcal{S} := \sum_w \mathcal{S}_w$, resp. $\tilde{\mathcal{S}} := \sum_w \tilde{\mathcal{S}}_w$).

Let $\omega_i := d\log(z - i)$, for $i = 0, 1$ and $\omega_p := d\log(z^p - 1)$.

Lemma 2.0.11. Let $f(z) = \sum_{1 \leq n} a_n z^n$, such that $df = \omega \sum_{1 \leq n} \gamma(\underline{s}; \underline{m})(n) z^n$.

If $\omega = \omega_0$ then $a_n = \gamma((s_1, \dots, s_k + 1); \underline{m})(n)$.

If $\omega = \omega_1$ then $a_n = -\sum_{0 \leq i \leq p-1} \gamma(\underline{s}, 1; \underline{m}, i)(n)$.

If $\omega = \omega_p$ then $a_n = -p\gamma(\underline{s}, 1; \underline{m}, m_k)(n)$.

Proof. Elementary computation. \square

Corollary 2.0.12. Suppose that $f(z) = \sum_{1 \leq n} q(n) z^n$, such that

$$df = \omega_i \sum_{1 \leq i} \alpha(n) z^n,$$

with $i = 0, 1$ or p and $\alpha \in \mathcal{S}_w$. Then $q \in \mathcal{S}_{w+1}$.

Remark 2.0.13. If $g(z) = \sum_{1 \leq n} k(n) z^n$, with $k \in \mathcal{F}_\sigma(\frac{1}{t})$, then we let $\mathbf{r}(g)(z) := \sum_{1 \leq n} \mathbf{r}(k)(n) z^n$. Similarly if $k \in \mathcal{F}(\frac{1}{t})$, then we let $\mathbf{s}(g)(z) := \sum_{1 \leq n} \mathbf{s}(k)(n) z^n$. Clearly, we have $\mathbf{r}(g') = \mathbf{r}(g)'$. On the other hand, in general $\mathbf{s}(g') \neq \mathbf{s}(g)'$. For example for $g(z) = \sum_{1 \leq n} \frac{z^n}{n}$, the left hand side is $\sum_{0 \leq n} z^n$, on the other hand the right hand side is $\sum_{\substack{0 \leq n \\ p \nmid (n+1)}} z^n$. However, if $\mathbf{s}(g') = f'$ for some $f = \sum_{1 \leq n} t(n) z^n$, with $t \in \mathcal{F}$, then $\mathbf{s}(g') = \mathbf{s}(g)'$. This follows from the basic observation that if $k(z)$ is a Laurent series such that $\mathbf{s}(zk(z)) = zt(z)$ for some power series $t(z)$, then the coefficient of $1/z$ in $k(z)$ is 0 and hence $\mathbf{s}(zk(z)) = z\mathbf{s}(k(z))$.

Proposition 2.0.14. Suppose that $f(z) = \sum_{1 \leq n} q(n) z^n$, such that

$$(2.0.1) \quad df = \omega_0 \sum_{1 \leq n} \alpha(n) z^n + \omega_1 \sum_{1 \leq n} \beta(n) z^n + \omega_p \sum_{1 \leq n} \gamma(n) z^n,$$

with $\alpha, \beta, \gamma \in \sum_{a+b=w} \mathcal{P}_a \cdot \tilde{\mathcal{S}}_b$. If $\lim_{n \rightarrow 0} q(n)$ exists then $q \in \sum_{a+b=w+1} \mathcal{P}_a \cdot \tilde{\mathcal{S}}_b$.

Proof. We have

$$nq(n) = \alpha(n) - \sum_{1 \leq k < n} \beta(k) - p \sum_{\substack{1 \leq k < n \\ p|(n-k)}} \gamma(k).$$

By Proposition 2.0.1, the function $nq(n)$ is a power series function and hence so is the function $q(n)$ when restricted to $\mathbb{N} \setminus p\mathbb{N}$. Let $r(z) := \sum_{0 \leq i} b_i z^i$ be the power series such that $nq(n) = r(n)$ for all $p|n$. The assumption on the limit implies that $\lim_{n \rightarrow 0} \frac{b_0}{n}$ exists. Hence $b_0 = 0$ and $q \in \mathcal{F}$.

By Corollary 2.0.12, there is $F(z) = \sum_{1 \leq n} s(n)z^n$ such that $s \in \sum_{a+b=w+1} \mathcal{P}_a \cdot \mathcal{S}_b$ and $\mathfrak{s} \circ \mathfrak{r}(F')dz$ is equal to the right hand side of (2.0.1), and hence $\mathfrak{s} \circ \mathfrak{r}(F') = f'$. Let $g = \mathfrak{r}(F)$. Then $\mathfrak{s}(g') = \mathfrak{s}(\mathfrak{r}(F')) = \mathfrak{s}(\mathfrak{r}(F')) = f'$. Since we proved above that $q \in \mathcal{F}$, we conclude by Remark 2.0.13 that $\mathfrak{s}(g') = \mathfrak{s}(g)'$. Therefore $\mathfrak{s}(g)' = f'$, and $f = \mathfrak{s}(g) = \mathfrak{s} \circ \mathfrak{r}(F)$. Hence q is of the form as stated above. \square

Proposition 2.0.15. \mathcal{P} is a \mathbb{Q} -algebra.

Proof. The statement follows from the shuffle product formula since this implies that $\mathcal{P}_a \cdot \mathcal{P}_b \subseteq \mathcal{P}_{a+b}$. \square

3. P-ADIC MULTI-ZETA VALUES

In this section we follow the notation of [4], except that we denote $g(z)$ by $\mathfrak{g}(z)$. Then letting $h := \mathcal{F}_*(t_{\infty 0} e_{t_{01}})$, we have $h = \mathfrak{g}(\infty)$. The fundamental equation [4, (2) p.135] that connects g and h takes the form:

$$(3.0.2) \quad (e_0 + e_1)h = h(e_0 + g^{-1}e_1g)$$

and the fundamental differential equation [4, (1) p.133] takes the form:

$$(3.0.3) \quad d\mathfrak{g} = p(e_0\mathfrak{g} - \mathfrak{g}e_0) \cdot \omega_0 + e_1\mathfrak{g} \cdot \mathcal{F}^*\omega_1 - p\mathfrak{g}(g^{-1}e_1g) \cdot \omega_1.$$

For every e^I , let $\mathfrak{g}[e^I]$ denote the coefficient of e^I in \mathfrak{g} and $\mathfrak{g}\{e^I\}$ denote the function that sends n to the coefficient of z^n in $\mathfrak{g}[e^I]$. If $I = e_0^{i_1} e_1^{j_1} \cdots e_0^{i_k} e_1^{j_k}$, let $d(I) := |\{j_t | j_t \neq 0, 1 \leq t \leq k\}|$ and $w(I) := \sum (i_t + j_t)$.

Theorem 3.0.16. For each I , $\mathfrak{g}\{e^I\} \in \sum_{a+b=w(I)} \mathcal{P}_a \cdot \tilde{\mathcal{S}}_b$ and $g[e^I] \in \mathcal{P}_{w(I)}$.

Proof. We will prove the statement by induction on $d(I)$.

Lemma 3.0.17. The statement above is true for $\mathfrak{g}\{e^I\}$, with $d(I) \leq 1$; for $\mathfrak{g}\{e_1 e_0^s e_1\}$, with any $s \geq 0$; and for $g[e^I]$, with $d(I) \leq 1$.

Proof. We proved on [4, p. 138] that $\mathfrak{g}\{e_0^{s-1} e_1\}(n) = \frac{p^s}{n^s}$, if $p \nmid n$ and 0 otherwise. Hence $\mathfrak{g}\{e_0^{s-1} e_1\} = p^s \sum_{1 \leq i < p} \gamma(s; i) \in \tilde{\mathcal{S}}_s$, since $\gamma(s; i) = \tilde{\gamma}(s; i)$, for $i \neq 0$. The statement for $\mathfrak{g}\{e^I\}$, with $d(I) \leq 1$, then follows from the fact that \mathfrak{g} is group-like.

Similarly, we proved on [4, p. 139] that $\mathfrak{g}\{e_1 e_0^{s-1} e_1\} =$

$$p^{s+1}((-1)^{s+1} \left(\sum_{\substack{0 \leq i, j < p \\ i \neq 0}} \gamma(s, 1; i, j) \right) - \sum_{\substack{0 \leq i < p \\ i \neq 0}} \gamma(s, 1; i, i)).$$

Clearly, when $i, j \neq 0$, $\gamma(a, b; i, j) = \tilde{\gamma}(a, b; i, j)$. Note that for $i \neq 0$, $\gamma(s, 1; i, 0)(n) = n^{-1} \sigma(s; i)(n)$, if $p|n$, and is 0 otherwise. Note that $\sigma(s; i)$ is a power series function

such that $\lim_{n \rightarrow 0} \sigma(s; i)(n) = 0$ [4, p. 139]. This implies that, for $p|n$, $\sigma(s; i)(n) = \sum_{1 \leq i} a_i n^i$, for some $a_i \in \mathbb{Q}_p$. Therefore $\gamma(s, 1; i, 0) = \tilde{\gamma}(s, 1; i, 0)$. Combining these, we deduce that $\mathfrak{g}\{e_1 e_0^{s-1} e_1\} \in \tilde{\mathcal{S}}_{s+1}$.

Finally, on [4, p. 140], we proved that $g[e_1] = 0$ and

$$g[e_0^{s-1} e_1] = \frac{p^s}{s-1} \sum_{0 < i < p} \sigma(s-1; i)^{(1)}(0),$$

for $s \geq 1$. Since $\sigma(s-1; i) = \tilde{\sigma}(s-1; i)$, the claim follows from Remark 2.0.9. To deduce the statement for all I with $d(I) \leq 1$, we use the fact that g is group-like [4]. \square

We will prove the result in several steps. Assume that we know the statement for:

- (i) $\mathfrak{g}\{e^I\}$, with $d(I) \leq k$;
- (ii) $\mathfrak{g}\{e_1 e_0^{s_k} e_1 \cdots e_0^{s_1} e_1\}$, for all $0 \leq s_i$; and
- (iii) $g[e^I]$, with $d(I) \leq k$.

Lemma 3.0.18. *For $d(I) \leq k+1$, $\mathfrak{g}\{e^I\} \in \sum_{a+b=w(I)} \mathcal{P}_a \cdot \tilde{\mathcal{S}}_b$.*

Proof. By (ii), we know the statement for $I = e_1 e_0^{s_k} e_1 \cdots e_0^{s_1} e_1$. It suffices to prove the statement for $e_0^{s_{k+1}} e_1 e_0^{s_k} e_1 \cdots e_0^{s_1} e_1$, and we will do this by induction on s_{k+1} . Assume that $\mathfrak{g}\{e_0^m e_1 e_0^{s_k} e_1 \cdots e_0^{s_1} e_1\} \in \sum_{a+b=w} \mathcal{P}_a \cdot \tilde{\mathcal{S}}_b$. Comparing the coefficient of $e_0^{m+1} e_1 e_0^{s_k} e_1 \cdots e_0^{s_1} e_1$ on both sides of (3.0.3), and using the inductive hypothesis, together with (i), (iii) and Proposition 2.0.15, we see that $d\mathfrak{g}[e_0^{m+1} e_1 e_0^{s_k} e_1 \cdots e_0^{s_1} e_1]$ is of the form as in the statement of Proposition 2.0.14. Furthermore, we note that $\lim_{n \rightarrow 0} \mathfrak{g}\{e_0^{m+1} e_1 e_0^{s_k} e_1 \cdots e_0^{s_1} e_1\}(n)$ exists [4, Proposition 2]. Therefore we can apply Proposition 2.0.14 to finish the proof. \square

Proposition 3.0.19. *If $d(I) \leq k+1$ then $h[e^I] \in \mathcal{P}_{w(I)}$.*

Proof. Note that $h[e^I] = \mathfrak{g}[e^I](\infty) = \lim_{n \rightarrow 0} \mathfrak{g}\{e^I\}(n)$. The statement then follows from Lemma 3.0.18, Remark 2.0.9, and Proposition 2.0.15. \square

The following simple lemma is crucial in what follows.

Lemma 3.0.20. *For $s_i \geq 0$, $g^{-1}[e_1 e_0^{s_{k+1}} \cdots e_1 e_0^{s_1}] + g[e_0^{s_{k+1}} e_1 \cdots e_0^{s_1} e_1] \in \mathcal{P}_w$, where $w = w(e_1 e_0^{s_{k+1}} \cdots e_1 e_0^{s_1})$.*

Proof. Let us compare the coefficient of $e_1 e_0^{s_{k+1}} \cdots e_1 e_0^{s_1} e_1$ on both sides of (3.0.2).

The left hand side is $h[e_0^{s_{k+1}} \cdots e_1 e_0^{s_1} e_1]$, which is in \mathcal{P}_w by the Proposition 3.0.19. The right hand side is $(g^{-1} e_1 g)[e_1 e_0^{s_{k+1}} \cdots e_1 e_0^{s_1} e_1]$, which is a sum of the expression in the statement of the lemma and sums of products of the form $g^{-1}[e^{I_1}]g[e^{I_2}]$ with $d(I_j) \leq k$, and $w(I_1) + w(I_2) = w$. The statement then follows from (iii) and Proposition 2.0.15. \square

Lemma 3.0.21. *For $s_i \geq 0$, $h[e_0^{s_{k+1}} e_1 e_0^{s_k} e_1 \cdots e_0^{s_1} e_1^2] + g[e_0^{s_{k+1}+1} e_1 \cdots e_0^{s_1} e_1] \in \mathcal{P}_{w+1}$, with w as above.*

Proof. Let us look at the coefficient of $e_0^{s_{k+1}+1} e_1 e_0^{s_k} e_1 \cdots e_0^{s_1} e_1^2$ with $s_i \geq 0$ in (3.0.2). The induction hypothesis, the fact that $h[e_0] = 0$, and Proposition 3.0.19, imply that $h[e_0^{s_{k+1}} e_1 e_0^{s_k} e_1 \cdots e_0^{s_1} e_1^2] = g^{-1}[e_0^{s_{k+1}+1} e_1 e_0^{s_k} e_1 \cdots e_0^{s_1} e_1] + (\text{terms in } \mathcal{P}_{w+1})$. Then using Lemma 3.0.20 we have the statement. \square

Lemma 3.0.22. *For every $s_i \geq 0$ there exist $t(\alpha_{k+1}, \dots, \alpha_1) \in \mathbb{Q}$, such that*

$$h[e_0^{s_{k+2}} e_1 \cdots e_0^{s_1} e_1] - \sum t(\alpha_{k+1}, \dots, \alpha_1) h[e_1 e_0^{\alpha_{k+1}} e_1 \cdots e_0^{\alpha_1} e_1]$$

is in \mathcal{P}_w , where $w = w(e_0^{s_{k+2}} e_1 \cdots e_0^{s_1} e_1)$ and the sum is over $\underline{\alpha} = (\alpha_{k+1}, \dots, \alpha_1)$ with $w(\underline{\alpha}) = \sum s_i$.

Proof. There is nothing to prove if $s_{k+2} = 0$, so we assume that $s_{k+2} > 0$. Looking at the coefficient of $e_0^{s_{k+2}} e_1 \cdots e_0^{s_1} e_1 e_0$ on both sides of (3.0.2), and using the induction hypotheses together with the fact that $h[e_0] = g[e_0] = 0$, we find that

$$h[e_0^{s_{k+2}-1} e_1 \cdots e_0^{s_1} e_1 e_0] - h[e_0^{s_{k+2}} e_1 \cdots e_0^{s_1} e_1] \in \mathcal{P}_w.$$

Next using the shuffle formula for $0 = h[e_0^{s_{k+2}-1} e_1 \cdots e_0^{s_1} e_1] h[e_0]$, and the above fact, we obtain that

$$(s_{k+2} + 1) h[e_0^{s_{k+2}} e_1 \cdots e_0^{s_1} e_1] + \sum_{1 \leq i \leq k+1} (s_i + 1) h[e_0^{s_{k+2}-1} e_1 \cdots e_0^{s_i+1} e_1 \cdots e_0^{s_1} e_1]$$

is in \mathcal{P}_w . From this the assertion follows by induction on s_{k+2} . \square

Lemma 3.0.23. *For $s_i \geq 0$, $\mathfrak{g}\{e_1 e_0^{s_{k+1}} e_1 e_0^{s_k} e_1 \cdots e_0^{s_1} e_1\} \in \tilde{\mathcal{S}}_w$, where we have $w = w(e_1 e_0^{s_{k+1}} e_1 e_0^{s_k} e_1 \cdots e_0^{s_1} e_1)$.*

Proof. Let us look at the coefficient of $e_1 e_0^{s_{k+1}} e_1 e_0^{s_k} e_1 \cdots e_0^{s_1} e_1$ in the differential equation (3.0.3) which gives $d\mathfrak{g}[e_1 e_0^{s_{k+1}} e_1 \cdots e_0^{s_1} e_1] =$

$$\mathfrak{g}[e_0^{s_{k+1}} e_1 \cdots e_0^{s_1} e_1] \cdot \mathcal{F}^* \omega_1 - p(\mathfrak{g}(g^{-1} e_1 g)) [e_1 e_0^{s_{k+1}} e_1 e_0^{s_k} e_1 \cdots e_0^{s_1} e_1] \cdot \omega_1.$$

By the induction all the terms contribute to give a term in the form that we are seeking except possibly the term $-p\omega_1(g^{-1}[e_1 e_0^{s_{k+1}} \cdots e_1 e_0^{s_1}] + g[e_0^{s_{k+1}} e_1 \cdots e_0^{s_1} e_1])$. But this is also in the form that we were looking for by Lemma 3.0.20. \square

Corollary 3.0.24. *For $s_i \geq 0$, $h[e_1 e_0^{s_{k+1}} e_1 \cdots e_0^{s_1} e_1] \in \mathcal{P}_w$, where we have $w = w(e_1 e_0^{s_{k+1}} e_1 \cdots e_0^{s_1} e_1)$.*

Proof. Clear using the fact that $h = \mathfrak{g}(\infty)$. \square

Lemma 3.0.25. *For $s_i \geq 0$, $g[e_0^{s_{k+1}+1} e_1 \cdots e_0^{s_1} e_1] \in \mathcal{P}_w$, where we have $w = w(e_0^{s_{k+1}+1} e_1 \cdots e_0^{s_1} e_1)$.*

Proof. This follows from combining Lemma 3.0.21, Lemma 3.0.22, and Corollary 3.0.24. \square

Lemma 3.0.26. *We have $g[e_1 e_0^{s_k} e_1 \cdots e_0^{s_1} e_1] \in \mathcal{P}_w$, with $w = w(e_1 e_0^{s_k} \cdots e_0^{s_1} e_1)$.*

Proof. If all $s_i = 0$, then the expression is 0. Otherwise let $j := \max\{i | s_i \neq 0\}$. Then applying Lemma 3.0.20 several times we see that it is sufficient to prove that $g[e_0^{s_j} e_1 \cdots e_0^{s_1} e_1^{k+2-j}] \in \mathcal{P}_w$, which we did in the previous proposition. \square

This finishes the proof of the theorem. \square

Recall that the p-adic multi-zeta values $\zeta_p(s_k, \dots, s_1)$ were defined as

$$(3.0.4) \quad g[e_0^{s_k-1} e_1 \cdots e_0^{s_1-1} e_1] = p^{\sum s_i} \zeta_p(s_k, \dots, s_1)$$

in [4, Definition 3].

Let \mathcal{Z} denote the \mathbb{Q} -space generated by the p-adic multi-zeta values. By the shuffle product formula this is an algebra.

Theorem 3.0.27. *We have the inclusion $\mathcal{Z} \subseteq \mathcal{P}$.*

Proof. This is a consequence of Theorem 3.0.16 and (3.0.4). \square

Remark 3.0.28. Furusho defined p -adic multiple-zeta values using Coleman's theory of iterated p -adic integrals. Our approach in [4] and here is based on Deligne's theory of the comparison isomorphism between the de Rham and the crystalline fundamental group. However, the \mathbb{Q} -space that these two different definitions generate are the same [2, Theorem 2.8, Examples 2.10] and hence the p -adic multiple-zeta values as defined by Furusho also lie in \mathcal{P} .

References

- [1] P. Deligne. *Le groupe fondamental de la droite projective moins trois points*. Galois Groups Over \mathbb{Q} , Ihara et. al., Editors (1989), 79-297.
- [2] H. Furusho. *p -adic multiple zeta values II. Tannakian interpretations*. Amer. J. Math. 129 (2007), no. 4, 1105-1144.
- [3] A. Goncharov. *Multiple polylogarithms and mixed Tate motives*. Preprint, AG/0103059v4.
- [4] S. Ünver. *p -adic multi-zeta values*. J. Number Theor. 108 (2004) 111-156.
- [5] S. Ünver. *Cyclotomic p -adic multi-zeta values in depth two*. Preprint.

KOÇ UNIVERSITY, MATHEMATICS DEPARTMENT. RUMELIFENERİ YOLU, 34450, İSTANBUL, TURKEY
E-mail address: `sunver@ku.edu.tr`